NASA Policy Directive

NPD 2810.1C
Effective Date: April 07, 2004
Expiration Date: June 30, 2009

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: NASA Information Security Policy

Responsible Office: Office of the Chief Information Officer

1. Policy

This NASA Policy Directive consolidates information security policy for both classified and unclassified information. Responsibility for information security is shared between the Office of the Chief Information Officer, which is responsible for unclassified information, and the Office of Security and Program Protection, which is responsible for classified information.

a. NASA shall protect all NASA information and associated Information Technology (IT) systems, both classified and unclassified, in a manner that is commensurate with the national security classification level, sensitivity, value, and criticality of the information.

b. All NASA information shall be protected from unauthorized disclosure, destruction, or modification while the information is being collected, processed, transmitted, stored, or disseminated.

c. NASA shall manage all classified and unclassified IT that is acquired, developed, or used in support of NASA missions, programs, projects, and institutional requirements by use of a process that covers the complete system life cycle.

d. NASA shall manage all IT in a cost-effective manner, guided by the application of sound risk management process that ensures an appropriate level of integrity, confidentiality, and availability of information in each phase of the life cycle of the system.

2. Applicability

a. This directive is applicable to NASA Headquarters and NASA Centers. This directive also applies to NASA Component Facilities and the Jet Propulsion Laboratory (JPL) to the extent specified in their contract. NASA employees, NASA contractors, and NASA grantees to the extent in their contract or grant must abide by the requirements of this directive when they perform work-related Agency missions, programs, projects, and institutional requirements. Facilities, resources, and personnel under a contract or grant from NASA at a college, university, or research establishment are included in the applicability of this directive.

b. For purposes of this directive, the following definitions apply:

(1) "Information" means any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by, or produced for, or is under the control of NASA.

(2) "Control" means the exercise of NASA's authority to regulate access to information.

(3) "Classified National Security Information (CNSI)" means information that has been determined pursuant to Executive Order (EO) 12958, as amended, or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(4) "Unclassified Information" means all information that does not meet the criteria described in EO 12958, as amended. Federal requirements for protecting unclassified information are prescribed in the Federal Information Security Management Act (FISMA) of 2002.

(5) "Systems" means a set of information resources under the same management control that share common functionality and require the same security needs.

(6) "National Security System" means any NASA IT system designated as being authorized to process CNSI.

3. Authority

a. 5 U.S.C. 552a, the Privacy Act of 1974, as amended.

b. 5 U.S.C. App. III, the Inspector General Act of 1978, as amended.

c. 18 U.S.C. 2510, The Wiretap Statute.

d. 18 U.S.C. 2701, the Electronic Communications Privacy Act (ECPA) of 1986, as amended.

e. 40 U.S.C. 1401, Information Technology Management Reform Act of 1996.

f. 40 U.S.C. 1441, the Computer Security Act of 1987, as amended.

g. 42 U.S.C. 2473 (c) (1), Section 203 (c) (1) of the National Aeronautics and Space Act of 1958, as amended.

h. 44 U.S.C. 3501, the Paperwork Reduction Act of 1995, as amended.

i. 44 U.S.C. 3541 et seq., Federal Information Security Management Act (FISMA) of 2002.

j. Executive Order (EO) 12958, Classified National Security Information, as amended (March 2003).

4. References

a. EO 13011, Federal Information Technology, July 16, 1996.

b. 32 CFR Part 2001, Information Security Oversight Office (ISOO) Directive No. 1, Classified National Security Information, October 13, 1999.

c. Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information Systems, June 5, 1999.

d. Index of National Security Telecommunications Information Systems Security Issuances (NSTISSI).

e. National Security Directive 42, National Policy for the Security of National Telecommunications and Information Systems, July 5, 1990.

f. NASA Procedural Requirements (NPR) 1000.2, NASA Strategic Management Handbook.

g. NASA Policy Directive (NPD) 1382.17, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulation.

h. NPD 1440.6, NASA Records Management.

i. NPR 1441.1, NASA Records Retention Schedule.

j. NPD 1600.2, NASA Security Policy.

k. NPR 1600.1, NASA Security Program Procedural Requirements.

l. NPD 1660.1, NASA Counterintelligence (CI) Policy

m. NPD 2800.1, Managing Information Technology.

n. NPR 2800.1, Managing Information Technology.

o. NPR 2810.1, Security of Information Technology.

p. NPD 7120.4, Program/Project Management.

q. NPR 7120.A, NASA Program and Project Management Processes and Requirements.

r. NPD 9800.1, NASA Office of Inspector General Programs.

s. NASA Standards, Series 2000, Computer Systems, Software, Data Systems.

5. Responsibility

a. The NASA Administrator shall:

(1) Be responsible for:

(i) Providing information security protections commensurate with the risk and magnitude of the harm resulting from

unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of NASA; and information systems used or operated by NASA or by a contractor of NASA or other organization on behalf of NASA;

(ii) Complying with the requirements of FISMA and related policies, procedures, standards, and guidelines for national security systems issued in accordance with law and as directed by the President; and (iii) Ensuring that information security management processes are integrated with NASA strategic and operational planning processes.

(2) Ensure that senior NASA officials provide information security for the information and information systems that support the operations and assets under their control through:

(i) Assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

(ii) Determining the levels of information security appropriate to protect such information and information systems for information security classifications and related requirements;

(iii) Implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and

(iv) Periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented.

(3) Delegate to the NASA Chief Information Officer (CIO) the authority to ensure compliance with the requirements imposed on NASA under FISMA sections 3541 et seq.

b. The NASA CIO shall:

(1) Develop and maintain an Agencywide information security program as required by FISMA. This will be accomplished by establishing and implementing information security and IT security policies and issuing instructions, memoranda, and bulletins designed to facilitate appropriate protection and accountability of information.

(2) Designate a senior Agency information security officer who shall:

(i) Carry out the Chief Information Officer's responsibilities for information security;

(ii) Possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) Have information security duties as that official's primary duty; and

(iv) Head an office with the mission and resources to assist in ensuring Agency compliance with FISMA section 3541 et seq.

(3) Ensure the development and maintenance of information security policies and procedures to protect unclassified information.

(4) Ensure the development and maintenance of a security certification program compliant with the National Institute of Standards and Technology guidelines for security Certifications and Accreditation of Federal information systems.

(5) Develop and maintain information security procedures and control techniques to address all applicable requirements of NASA's unclassified information technology security program.

(6) Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.

(7) Issue interim guidance, regarding protection and management of unclassified information and IT resources, in the form of NASA Information Technology Requirement (NITR) as necessary to keep pace with the dynamic IT security environment.

(8) Charter a NASA Competency Center for IT Security to provide advice and assistance to the NASA CIO regarding IT Security Policy and technical issues; assist Centers in implementing policy, procedures, and guidelines; investigate new security hardware and software tools; establish working groups and expert centers, as necessary, to support information security initiatives.

(9) In coordination with the Office of Security and Program Protection, ensure procedures are established for the referral of reports of computer crimes involving information systems to the NASA Office of Inspector General (OIG) in a timely manner. Computer crimes include unauthorized access of information, compromises of computers, and other IT resources such as telecommunications systems, command and control systems, and network systems for investigation.

c. The NASA Office of Security and Program Protection shall:

(1) In collaboration with the CIO, develop and implement information security procedural requirements, memoranda,

and bulletins for NASA designed to direct and facilitate the protection of both classified and sensitive but unclassified information (also referred to as Administratively Controlled Information).

(2) Establish a program with multiple security disciplines (e.g., physical, personnel, industrial, communications security (COMSEC), and emanations security (TEMPEST)) for the oversight and protection of classified national security information (CNSI) to include Certification and Accreditation of national security systems in compliance with the National Information Assurance Certification and Accreditation Process.

(3) Establish a NASA COMSEC Material Control System (CMCS) and appoint a Central Office of Record (COR), which shall set forth minimum National Security Agency standards, procedures, specifications, and guidelines for safeguarding and controlling COMSEC material in NASA's possession. The COR shall investigate and monitor COMSEC incidents.

(4) Establish a NASA Information Assurance Office with the mission and resources to:

(i) Develop and implement an information security review program designed to ensure that all NASA information systems used to process both unclassified and classified information are in compliance with NASA policy, NASA procedural requirements, and with Federal guidelines. Information security reviews shall be coordinated with the NASA OIG Office of Audits to ensure that the review efforts are not duplicated.

(ii) Assure that information security certification is conducted for each information system per the National Institute of Standards and Technology guidance to assure comprehensive evaluation of management, operational, and technical controls.

(iii) Establish and oversee an information management process to identify, categorize, and label critical systems and information according to the National Institute of Standards and Technology guidelines for information labeling.

(5) Coordinate the initial assessment of suspected computer crimes such as unauthorized access of information, compromises of computers, and other IT resources, such as telecommunications systems, command and control systems, and network systems, with the CIO, the OIG, and other organizations or agencies as appropriate.

(6) In accordance with NPR 1600.1 establish policy, procedural requirements, and budget for appropriate security background investigations of persons who require access to IT systems, applications, and networks operated by or on behalf of NASA.

(7) Conduct counterintelligence reviews, threat assessments and investigations, and issue threat bulletins for NASA to protect both classified and unclassified information.

(8) Conduct the appropriate investigations into computer incidents involving classified systems.

d. The Associate Administrators for the Enterprise Offices and the Assistant Administrators for the Institutional Program Offices will perform the following:

(1) Participate with the Office of Security and Program Protection and the NASA CIO in their respective development of NASA information security and IT security policies, standards, best practices, and guidance that protects NASA information and IT assets.

(2) Apply these policies and requirements, consistent with sound systems engineering and prudent risk management practices, for encryption and embedded software (e.g., IT in spacecraft, aircraft, satellites, facility and system monitoring equipment, and test equipment to include uplink, downlink, and crosslink command and communications) throughout its life cycle and for other embedded IT, through design, development, test and evaluation, until and through deployment.

(3) Ensure that sufficient resources are allocated to address information security and IT security requirements developed under this directive.

(4) Ensure that their respective organizations and assigned Centers, including missions, programs, projects, and institutions under their purview, comply with this directive.

(5) Ensure that adequate information security and IT security risk management design and planning is conducted to allow for effective cost- benefit analyses of alternate information security postures and of risk acceptance.

e. The OIG shall be responsible for the investigation of all computer security crimes, such as unauthorized access of information systems, compromises of computers and other information technology resources such as telecommunications systems, command and control systems, and network systems.

f. The Center Directors and the Director for Headquarters Operations will perform the following:

(1) Ensure compliance with this directive, NASA policies, procedures, requirements, and Federal information security policy.

(2) Appoint a Center IT Security Manager to assist the Center CIO to implement this directive, NASA IT security

policies and procedures, and Federal IT security laws and regulations.

(3) Ensure the Center CIO has adequate staff, resources, budget, and authority to implement the information security programs.

(4) Establish a Center Network Configuration Control Board to ensure that Center networks are managed, that information security requirements are implemented and enforced, and that exceptions are reviewed and justified before being approved and implemented.

(5) Make available qualified personnel to support periodic assessments conducted by the Office of Security and Program Protection.

g. Center CIOs and the Headquarters Operations CIO shall be responsible and accountable for the protection of information and the IT resources under their cognizance and for compliance with this directive, NASA information security policies, NASA procedural requirements, and Federal information security policy.

h. Center Chiefs of Security and the Headquarters Chief of Security shall be responsible for the coordination of investigations of information security incidents. Referral of an information security incident to an investigating authority shall be made in consultation with the Center CIO. Center Chiefs of Security and the Headquarters Chief of Security will cooperate and assist, as requested, by NASA OIG in its investigation of computer crimes.

6. Delegation of Authority

The NASA Chief Information Officer is authorized to ensure compliance with the requirements imposed on the Agency under FISMA subchapter 3544.

7. Measurements

The effectiveness of this directive will be assessed as follows:

a. Measurements will be collected and evaluated by the NASA CIO to assess the effectiveness of this policy directive at least annually by measuring the degree of compliance with assignments of responsibility for security, establishment of security plans, review of security controls, and documented authorizations that security plans are adequately implemented.

b. Measurements will be collected and evaluated by the NASA CIO at least annually to assess trends involving security incidents and trends for tracking metrics involving the cost, schedule impact, and affect on mission, program, and project performance attributed to the loss, alteration, unavailability, misuse, or unauthorized access to or modification of Agency information or IT resources.

8. Cancellation

NPD 2810.1, Security of Information Technology, dated October 1, 1998.

/s/ Sean O'Keefe
Administrator

Attachment A: (Text)

None.

(URL for Graphic)

None.

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: http://nodis3.gsfc.nasa.gov

NPD 2810.1C -- TOC
Verify Current version before use at:
http://nodis3.gsfc.nasa.gov/
Page 6 of 6